【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成20年9月18日(2008.9.18)

【公表番号】特表2008-524886(P2008-524886A)
【公表日】平成20年7月10日(2008.7.10)
【年通号数】公開・登録公報2008-027
【出願番号】特願2007-546014(P2007-546014)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｇ０６Ｋ　19/10　(2006.01)
Ｇ０６Ｋ　17/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ａ
Ｇ０６Ｋ　19/00　Ｒ
Ｇ０６Ｋ　17/00　Ｔ

【手続補正書】
【提出日】平成20年7月31日(2008.7.31)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
システム・ユニットと、
前記システム・ユニットに結合された媒体読取装置と、
前記媒体読取装置を制御するためのデバイス・ドライバと、
前記媒体読取装置により読み取り可能な取り外し可能記憶媒体であって、第１の非対称暗号鍵ペアに対応する第１の秘密鍵と第２の非対称暗号鍵ペアに対応する第１の公開鍵とを保管する取り外し可能記憶媒体と、
前記システム・ユニットに結合されたハードウェア・セキュリティ・ユニットであって、前記第２の非対称暗号鍵ペアに対応する第２の秘密鍵と前記第１の非対称暗号鍵ペアに対応する第２の公開鍵とを保管し、
前記第１および第２の暗号鍵ペアに基づいて前記取り外し可能記憶媒体および前記ハードウェア・セキュリティ・ユニットを認証するためのロジックと、
前記取り外し可能記憶媒体および前記ハードウェア・セキュリティ・ユニットが相互に認証された後、前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記システム・ユニットが前記ハードウェア・セキュリティ・ユニット上の暗号機能を呼び出せるようにするためのロジックと、
を有するハードウェア・セキュリティ・ユニットと、
を有する、データ処理システム。
【請求項２】
前記取り外し可能記憶媒体が認証され、前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままであるときに、アプリケーションを認証するためのロジックをさらに有する、請求項１に記載のデータ処理システム。
【請求項３】
前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記ハードウェア・セキュリティ・ユニットにより前記取り外し可能記憶媒体に関するデジタル証明

書を生成するためのロジックをさらに有する、請求項１または２に記載のデータ処理システム。
【請求項４】
前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記デバイス・ドライバからの要求に応答して前記ハードウェア・セキュリティ・ユニットにより前記デバイス・ドライバからのデータ項目にデジタル署名を行うためのロジックをさらに有する、請求項１、２、または３に記載のデータ処理システム。
【請求項５】
前記取り外し可能記憶媒体が前記媒体読取装置に連結される必要なしに前記取り外し可能記憶媒体と前記ハードウェア・セキュリティ・ユニットとの間の相互認証動作を正常に実行した後、前記デバイス・ドライバからの要求に応答して前記デバイス・ドライバのために前記ハードウェア・セキュリティ・ユニットにより暗号機能を実行するためのロジックをさらに有する、請求項１ないし４のいずれかに記載のデータ処理システム。
【請求項６】
前記デバイス・ドライバが、
第３の非対称暗号鍵ペアに対応する第３の秘密鍵と、
第４の非対称暗号鍵ペアに対応する第３の公開鍵と、
を有し、
前記データ処理システムが、
前記ハードウェア・セキュリティ・ユニット上に保管され、前記第４の非対称暗号鍵ペアに対応する第４の秘密鍵と、前記第３の非対称暗号鍵ペアに対応する第４の公開鍵と、
前記第３および第４の非対称暗号鍵ペアに基づいて前記デバイス・ドライバと前記ハードウェア・セキュリティ・ユニットとの間の相互認証動作を実行するためのロジックと、
前記取り外し可能記憶媒体および前記デバイス・ドライバが相互に認証された後、前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記デバイス・ドライバが前記ハードウェア・セキュリティ・ユニット上の機能を呼び出せるようにするためのロジックと、
をさらに有する、請求項１ないし５のいずれかに記載のデータ処理システム。
【請求項７】
前記取り外し可能記憶媒体および前記デバイス・ドライバが認証され、前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままであるときに、アプリケーションを認証するためのロジックをさらに有する、請求項６に記載のデータ処理システム。
【請求項８】
前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記ハードウェア・セキュリティ・ユニットにより前記デバイス・ドライバに関するデジタル証明書を生成するためのロジックをさらに有する、請求項６または７に記載のデータ処理システム。
【請求項９】
暗号機能を実行するための方法であって、
システム・ユニットに結合された媒体読取装置に取り外し可能記憶媒体を連結するステップであって、
前記システム・ユニットがハードウェア・セキュリティ・ユニットと前記媒体読取装置を制御するためのデバイス・ドライバとを含み、
前記取り外し可能記憶媒体が第１の非対称暗号鍵ペアに対応する第１の秘密鍵と第２の非対称暗号鍵ペアに対応する第１の公開鍵とを含み、
前記ハードウェア・セキュリティ・ユニットが前記第２の非対称暗号鍵ペアに対応する第２の秘密鍵と前記第１の非対称暗号鍵ペアに対応する第２の公開鍵とを含むステップと、

前記第１および第２の非対称暗号鍵ペアに基づいて前記取り外し可能記憶媒体と前記ハードウェア・セキュリティ・ユニットとの間の相互認証動作を実行するステップと、
前記相互認証動作を正常に実行したことに応答して、前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記システム・ユニットが前記ハードウェア・セキュリティ・ユニット上の暗号機能を呼び出せるようにするステップと、
を含む、方法。
【請求項１０】
暗号機能を実行するためにデータ処理システム内で使用するためのコンピュータ可読媒体上のコンピュータ・プログラムであって、
前記コンピュータ可読媒体上に保管され、システム・ユニットに結合された媒体読取装置により取り外し可能記憶媒体を読み取るためのロジックであって、
前記システム・ユニットがハードウェア・セキュリティ・ユニットと前記媒体読取装置を制御するためのデバイス・ドライバとを含み、
前記取り外し可能記憶媒体が第１の非対称暗号鍵ペアに対応する第１の秘密鍵と第２の非対称暗号鍵ペアに対応する第１の公開鍵とを含み、
前記ハードウェア・セキュリティ・ユニットが前記第２の非対称暗号鍵ペアに対応する第２の秘密鍵と前記第１の非対称暗号鍵ペアに対応する第２の公開鍵とを含むロジックと、
前記コンピュータ可読媒体上に保管され、前記取り外し可能記憶媒体が前記媒体読取装置に連結されている間に前記媒体読取装置と前記ハードウェア・セキュリティ・ユニットとの間の相互認証動作を実行するためのロジックと、
前記コンピュータ可読媒体上に保管され、前記取り外し可能記憶媒体と前記ハードウェア・セキュリティ・ユニットとの間の前記相互認証動作を正常に実行したことに応答して、前記取り外し可能記憶媒体が前記媒体読取装置に連結されたままである間に前記ハードウェア・セキュリティ・ユニット上の暗号機能を使用可能にするためのロジックと、
を含む、コンピュータ・プログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】暗号機能を実行するためのデータ処理システム、方法、およびコンピュータ・プログラム
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００２
【補正方法】変更
【補正の内容】
【０００２】
本出願は、２００４年１月８日に出願され、「Ｍｅｔｈｏｄ ａｎｄ ｓｙｓｔｅｍ ｆｏｒ ｅｓｔａｂｌｉｓｈｉｎｇ ａ ｔｒｕｓｔ ｆｒａｍｅｗｏｒｋ ｂａｓｅｄ ｏｎ ｓｍａｒｔ ｋｅｙ ｄｅｖｉｃｅｓ」という発明の名称の米国特許出願公報第２００５／０１５４８７５号、ならびに２００４年１月８日に出願され、「Ｍｅｔｈｏｄ ａｎｄ Ｓｙｓｔｅｍ ｆｏｒ Ｐｒｏｔｅｃｔｉｎｇ Ｍａｓｔｅｒ Ｓｅｃｒｅｔｓ Ｕｓｉｎｇ Ｓｍａｒｔ Ｋｅｙ Ｄｅｖｉｃｅｓ」という発明の名称の米国特許出願公報第２００５／０１５４８９８号に関連する。